AMENDMENTS TO THE CLAIMS

The following claims are respectfully submitted for consideration along with the current claims in the application:

Listing of Claims

1. (Previously Presented) An apparatus for protecting a computer system, comprising: a password controller coupled to said computer system, said password controller capable of receiving a password attempt and capable of operating a computer program to compare said password attempt with a stored password, wherein said stored password comprises a password segment and said password segment comprises: an entry event comprising a predetermined entry signal; a predetermined time interval following said entry event; and a terminating signal following said predetermined time interval, said terminating signal marking the end of said password segment; wherein said computer program is capable of allowing access to said computer system when a password segment of said password attempt matches said password segment of said stored password.

2. (Previously Presented) The apparatus as set forth in claim 1 wherein said computer program is capable of comparing a time envelope of said stored password with a time envelope of a received password attempt, and capable of denying access to said computer system when said time envelope of said received password attempt does not match said time envelope of said stored password.

3. (Previously Presented) The apparatus as set forth in claim 1 wherein said computer program compares said stored password with said password attempt received from an online connection to determine whether said password attempt from said online connection matches said stored password.

4. (Previously Presented) The apparatus as set forth in claim 1 wherein said entry event comprises a predetermined combination of computer readable entry signals, wherein each computer readable entry signal comprises one of: a character, a symbol, and a number.

5. (Previously Presented) The apparatus as set forth in claim 1 wherein said terminating signal is an entry event that follows said predetermined time interval.

6. (Previously Presented) The apparatus as set forth in claim 3 wherein said computer program is capable of sending a signal to said online connection that indicates whether said password attempt received from said online connection matches said stored password.

7. (Previously Presented) The apparatus as set forth in claim 6 wherein computer program is capable of waiting until a time delay period expires before sending said signal that indicates whether said password attempt received from said online connection matches said stored password.

8. (Previously Presented) The apparatus as set forth in claim 7 wherein said time delay period is of variable duration.

9. (Previously Presented) The apparatus as set forth in claim 1 wherein said stored password comprises at least one password segment comprising a predetermined time interval calculated by subtracting from the total time measured from the trailing edge of a first entry event to the trailing edge of a next second entry event the time required to read said next second entry event.

10. (Previously Presented) The apparatus as set forth in claim 2 wherein said stored password further comprises a plurality of password segments wherein the total time of said plurality of password segments equals said time envelope of said stored password, within a predetermined deviation.

11. (Previously Presented) An apparatus for protecting a computer system, comprising: a password controller coupled to said computer system, said password controller capable of receiving a password attempt and capable of operating a computer program to compare a time envelope of a received password attempt with a time envelope of a stored password, and capable of denying access to said computer system when said time envelope of said received password attempt does not match said time envelope of said stored password.

12. (Previously Presented) A method of protecting an computer system, comprising the steps of: detecting an initial entry event of a password attempt; determining whether a password segment of said password attempt matches a password segment of a stored password wherein said password segment comprises: an entry event comprising a predetermined entry signal; a predetermined time interval following said entry event; and a terminating signal following said predetermined time interval, said terminating signal marking the end of said password segment; and allowing access to said computer system when said password segment of said password attempt matches said password segment of said stored password.

13. (Previously Presented) The method as set forth in claim 12 further comprising the step of: calculating a time interval of said password segment of said password attempt by subtracting the time required to read a next second entry event from the total time measured from the trailing edge of a first entry event to the trailing edge of said next second entry event; and determining whether said time interval of said password segment of said password attempt matches a time interval of said password segment of said stored password.

14. (Previously Presented) The method as set forth in claim 13 further comprising the steps of: waiting for a time delay period to expire after determining whether said password attempt matches said stored password; and sending a signal that indicates whether said password attempt matches said stored password.

15. (Previously Presented) The method as set forth in claim 14 wherein said time delay period is of variable duration.

16. (Previously Presented) The method as set forth in claim 13 further comprising the step of: determining whether said entry event of each said password segment of said password attempt matches a corresponding entry event of said password segment of said stored password.

17. (Previously Presented) The method as set forth in claim 13 further comprising the step of: determining whether said time interval of said password segment of said password attempt matches a corresponding time interval of each said password segment of said stored password.

18. (Previously Presented) The method as set forth in claim 12 further comprising the step of: comparing each entry signal in said entry event in said password segment of said password attempt with a corresponding entry signal in said entry event of said password segment of said stored password.

19. (Previously Presented) The method as set forth in claim 12 further comprising the step of: beginning the timing of said password segment of said password attempt at the trailing edge of one of a first entry event and first entry signal; and concluding the timing of said password segment of said password attempt at the trailing edge of one of a next second entry event and next second entry signal.

20. (Previously Presented) A method of protecting an computer system comprising the steps of: detecting an initial entry event of a password attempt; comparing a password segment of said password attempt to a password segment of a stored password; determining whether said password attempt matches said stored password; waiting for a time delay period to expire after determining whether said

password attempt matches said stored password; and allowing access to said computer system when said password attempt matches said stored password.

21. (Previously Presented) The method as set forth in claim 19 further comprising the steps of: comparing a time envelope of said stored password to a time envelope of said password attempt; determining whether a time interval of a password segment of said password attempt matches a corresponding time interval of said password segment of said stored password; and calculating a time interval of said password segment of said password attempt by subtracting the time required to read a next second entry event from the total time measured from the trailing edge of a first entry event to the trailing edge of said next second entry event.

22. (Previously Presented) For use in a computer, computer executable process steps stored on a computer readable storage medium capable of protecting said computer, comprising the steps of: detecting an initial entry event of a password attempt; determining whether a password segment of said password attempt matches a password segment of a stored password wherein said password segment comprises: an entry event comprising a predetermined entry signal; a predetermined time interval following said entry event; and a terminating signal following said predetermined time interval, said terminating signal marking the end of said password segment; and allowing access to said computer system when said segment of said password attempt matches said password segment of said stored password.

23. (Previously Presented) The computer executable process steps stored on a computer readable storage medium, as set forth in claim 22, further comprising the steps of: calculating a time interval of said password segment of said password attempt by subtracting the time required to read a next second entry event from the total time measured from the trailing edge of a first entry event to the trailing edge of said next second entry event; and determining whether said time interval of said password segment of said password attempt matches a time interval of said password segment of said stored password.

24. (Previously Presented) The computer executable process steps stored on a computer readable storage medium, as set forth in claim 22 further comprising the steps of: waiting for a time delay period to expire after determining whether said password attempt matches said stored password; and sending a signal that indicates whether said password attempt matches said stored password.

25. (Previously Presented) The computer executable process steps stored on a computer readable storage medium, as set forth in claim 22, further comprising the step of: waiting an arbitrary and variable time delay period before sending said signal that indicates whether said password attempt signals matches said stored password.

26. (Previously Presented) The computer executable process steps stored on a computer readable storage medium, as set forth in claim 22 further comprising the step of: determining whether said entry event of each said password segment of said password attempt matches a corresponding entry event of said password segment of said stored password.

27. (Previously Presented) The computer executable process steps stored on a computer readable storage medium, as set forth in claim 22 further comprising the step of: determining whether said time interval of said password segment of said password attempt matches a corresponding time interval of each said password segment of said stored password.

28. (Previously Presented) The computer executable process steps stored on a computer readable storage medium, as set forth in claim 21 further comprising the step of: comparing each entry signal in said entry event in said password segment of said password attempt with a corresponding entry signal in said entry event of said password segment of said stored password.

29. (Previously Presented) The computer executable process steps stored on a computer readable storage medium, as set forth in claim 22 further comprising the step of: beginning the timing of said password segment of said password attempt at the trailing edge of one of a first entry event and first entry signal; and concluding the timing of said password segment of said password attempt at the trailing edge of one of a next second entry event and next second entry signal.

30. (New) A method of authenticating a user device, said method comprising the steps of:

receiving by an authentication device, a password sent from the user device, said password comprising a sequence of predefined characters, each of said characters being separated by a predefined time interval from an adjacent character in the sequence;

determining by the authentication device, whether the received characters match the predefined characters;

determining by the authentication device, whether the received time interval between the received characters matches the predefined time interval; and

positively authenticating the user device only if the received characters match the predefined characters, and the received time interval between the received characters matches the predefined time interval.

31. (New) The method of claim 30, wherein the predefined time interval between a first pair of characters is different than the predefined time interval between a second pair of characters.

32. (New) The method of claim 30, wherein the step of determining whether the received time interval between the received characters matches the predefined time interval includes:

measuring the time interval between the received characters; and

determining whether the measured time interval is within a predefined positive or negative tolerance value of the predefined time interval.

33. (New) The method of claim 30, further comprising waiting for an arbitrary time period after the authenticating step is complete before sending an authorization message from the authentication device to the user device.

34. (New) The method of claim 30, further comprising sending information regarding the predefined time interval from the authentication device to the user device.

35. (New) The method of claim 34, wherein the authentication device periodically sends a new time interval to the user device.

36. (New) The method of claim 30, wherein the user device is a magnetic card reader, and the authentication device is a server in a financial authorization network.

37. (New) The method of claim 30, wherein the user device is a magnetic card reader, and the authentication device is a connected to a server in a financial authorization network.

38. (New) In a user device, a method of constructing a password utilized by an authentication device to authenticate the user device, said method comprising the steps of:

forming a sequence of predefined characters; and

separating each of said characters from an adjacent character in the sequence by a predefined time interval.

39. (New) The method of claim 38, wherein the forming step includes forming a sequence of at least three characters, and wherein the predefined time interval between a first pair of characters is different than the predefined time interval between a second pair of characters.